

# The Future Of Defense

## IT Leaders Brace for Unprecedented Cyber Threats

With artificial intelligence fueling an explosion in threats, cybercriminals are adding sophisticated new weapons to their arsenals. As technology continues to advance, constant adaptation by IT and security leaders is critical to combat these evolving threats. Keeper Security commissioned an independent research agency to survey over 800 leaders around the globe about the modern digital landscape.

### ORGANIZATIONS UNDER FIRE

92%

of IT leaders say cyber attacks are more frequent today than a year ago

### UNPRECEDENTED THREATS

95%

of IT leaders report that cyber attacks are more sophisticated than ever before

### LEADERS REMAIN FOCUSED

92%

of IT and security leaders say that cybersecurity is their number one priority

### Cyber attacks that are increasing, according to IT leaders

1



51%  
Phishing

2



49%  
Malware

3



44%  
Ransomware

4



31%  
Password Attacks

5



28%  
DoS

### Emerging attack vectors IT leaders are witnessing

51%

AI-Powered Attacks



35%

AI-Powered Attacks

36%

Deepfake Technology



30%

Deepfake Technology

36%

Supply Chain Attacks



29%

5G Network Exploits

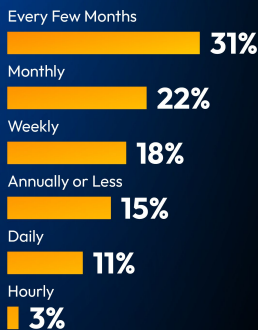


Cybersecurity fundamentals are the bedrock of our digital fortitude. As threats evolve, these fundamentals act as our first line of defense, providing a robust and proactive shield against existing and emerging risks. Prioritizing these basics is not just a strategy; it's a necessity.

**Darren Guccione**  
CEO and Co-founder,  
Keeper Security



### IT Leaders Navigate Waves of Attacks



Despite an evolving threat landscape, the fundamental rules of protecting an organization remain relevant. Organizations should prioritize adoption of password and Privileged Access Management (PAM) solutions that protect against the most prevalent cyber attacks. A password manager mitigates risk by enforcing strong password practices, while PAM safeguards an organization's vital assets by controlling and monitoring high-level access, collectively fortifying defenses and minimizing potential damage in the event that a successful cyber attack does occur.